

# **ELECTRONIC CERTIFICATE, METHOD, APPARATUS AND PROGRAM FOR ISSUING AND VERIFYING ELECTRONIC CERTIFICATE, AND RECORDING MEDIUM FOR PROGRAM**

**Publication number:** JP2003258787 (A)

**Publication date:** 2003-09-12

**Inventor(s):** IIDA TAKAHIRO; UENO MASAMI; AGAWA YUSUKE; KITO TOSHIYUKI +

**Applicant(s):** NIPPON TELEGRAPH & TELEPHONE +

**Classification:**

- international: **G06Q10/00; G06Q50/00; H04L9/08; G06Q10/00; G06Q50/00; H04L9/08;** (IPC1-7): G06F17/60; H04L9/08

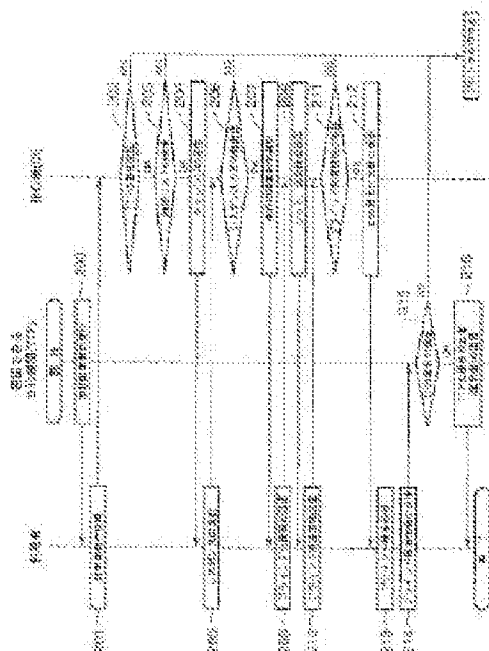
- European:

**Application number:** JP20020050053 20020226

**Priority number(s):** JP20020050053 20020226

## **Abstract of JP 2003258787 (A)**

**PROBLEM TO BE SOLVED:** To provide a method for issuing an electronic certificate by which the load of a anonymous authentication system can be reduced and anonymous authentication services can be provided without damaging security even with respect to conspiracy of any subject except for a reliable public institution. ; **SOLUTION:** A public institution device TTP verifies the digital signature of a publisher from blind decompressed information acquired by implementing a prescribed calculation on the digital signature due to a publisher device transmitted from a user device by a prescribed calculation, and the digital signature of the public institution device TTP is implemented on the blind decompressed information and transmitted to the user device as the electronic certificate. ;  
COPYRIGHT: (C)2003,JPO



Data supplied from the **espacenet** database — Worldwide